The official voice of the Air Force Research Laboratory
news@afrl
Roundups
September 2001

Secure information network goal of AFRL's Rome site

by Fran Crumb, Information Directorate

ROME, N.Y. — A secure, fiber-optic computer network is the goal of a $3,938,051 contract awarded by the Air Force Research Laboratory Information Directorate to BBNT Solutions of Cambridge, Mass.

The two-year contract, "Building the Quantum Network," is funded by the Defense Advanced Research Projects Agency of Arlington, Va., under its Quantum Information Science and Technology (QuIST) program. QuIST seeks innovative research both in underlying information technology and in scalable component technology for quantum information systems. The goal is to demonstrate the potential for practical use of quantum effects in communication and computation. DARPA is primarily interested in projects that offer simultaneous advances in underlying ideas, algorithms, architectures, and scalable components.

"BBNT engineers will be developing cyber network testbeds for distributing security cryptography keys," said Dr. Donald J. Nicholson, program manager in the directorate's Information Grid Division. The ultimate goal of research under this contract is a physically assured, secure information network. The technology could eventually have numerous civilian applications, since it will protect information being transferred via an internet."

Nicholson said the agreement covers the first two years of the five-year QuIST program. BBNT will subcontract with Boston University and Harvard University to design and build the world's first Quantum Network, delivering end-to-end network security via high-speed Quantum Key Distribution. Researchers will also test that network against sophisticated eavesdropping attacks. As an option, an ultra-high-security network will be fielded through commercial fiber optic lines across the metro Boston area and operated between Boston University, Harvard and BBNT.

The quantum network will provide extremely high levels of communications security for high-speed data streams and will be fully compatible with the standard Internet architecture. Security will be based on physical laws rather than classic public or secret key techniques and will remove any concerns about traffic compromise due to the possible vulnerabilities of public key cryptography. **@**